

In re: Hind et al.
Application No.: 09/765,127
Filed: January 17, 2001
Page 19

REMARKS

The Applicants appreciate the thorough examination of the current application as evidenced by the Final Office Action dated July 12, 2005 (the "Action").

The above amendments have been made to address the claim objections on page 3 of the Action. Entry of these amendments is requested as no new issues have been raised. In particular, the Applicants have merely corrected informalities noted by the Examiner

In the following remarks, the Applicants will show that all claims are patentable over the cited references. A Notice of Allowance is respectfully requested in due course.

Claim 1 is Patentable Over the Cited References

Claim 1 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,640,145 to Hoffberg et al. ("Hoffberg") in view of U.S. Publication No. 2002/0029350 to Cooper et al. ("Cooper") and in further view of U.S. Publication No. 2002/0080967 to Abdo ("Abdo"). In response, Applicants will show that Claim 1 is patentable for at least the reasons discussed below.

Applicants respectfully submit that the portions of Abdo relied upon in the Action are not supported by the earliest priority document of Abdo, and therefore the relied-upon portions of Abdo are not prior art under § 102(e).

Specifically, Abdo claims priority to Provisional Application Nos. 60/258,843, filed Dec. 27, 2000, and 60/300,563, filed on June 22, 2001. The current application was filed January 17, 2001. Therefore, only Provisional Application No. 60/258,843 was filed prior to the current application, and any portions of Abdo relied upon must be supported by Provisional Application No. 60/258,843 to be considered prior art under § 102(e) with respect to the current application. A copy of Provisional Application No. 60/258,843 from the image file wrapper of Abdo (reproduced from the USPTO public PAIR online system) is attached. Secured links or modes are discussed in Provisional Application No. 60/258,843 on page 1, paragraph 7; page 2, paragraph 8; page 3, paragraphs 1 and 5 (which continues on page 4). Applicants fail to find support in Provisional Application No. 60/258,843 for the portions of Abdo discussed on page 6 of the Action. If the current rejection is maintained, the Examiner

is respectfully requested to point out the specific portions of Provisional Application No. 60/258,843 which are relied upon to support the rejection.

Applicants submit that a Declaration under Rule 132 showing prior invention is not necessary at this time and is not submitted herewith. However, should the Examiner maintain the rejection based on Abdo provisional application of December 27, 2000, Applicants reserve the right to submit such a Declaration at that time.

In the alternative, Applicants submit that even if support can be found in the Abdo provisional application of December 27, 2000, the current claims are patentable over the cited references. In particular, Claim 1 recites, in part:

wherein the security core is configured to detect whether the audio recording component and the at least one transformation component remain operably connected to the security core during the recording and the transforming of the audio stream; and

wherein the security core is configured to abort the recording and the transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording and the transforming of the audio stream.

Applicants respectfully submit that the cited references, taken alone or in combination, fail to teach or suggest at least a security core that is configured to abort the recording and the transforming if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording of the audio stream and the transforming of the audio stream.

The Action concedes that Hoffburg and Cooper lack these recitations. However, the Action states that Abdo teaches a wireless secure device that includes these recitations and cites paragraphs 6, 9-11, and 86 of Abdo. *See* page 6 of the Action.

Applicants respectfully disagree with the characterization of Abdo in the Action. In particular, the cited portions of Abdo discuss warning the user if the security mode is switched off without permission being granted. *See* Abdo at Paragraph 11 ("informing a user of the status of the data link (e.g., normal link (mode) or secured link (mode)), and [for] warning the user if the security mode is switched off without permission being granted." (emphasis added)). In contrast, Claim 1 recites a security core that is configured to abort the

recording and the transforming of the audio stream if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core. Nothing in Abdo teaches or suggests this feature.

Abdo discusses in paragraph 73 that "[i]f the connection switches from SECURE mode to NORMAL mode without the user providing the requisite information, the system 101 will provide a warning back to the user." Abdo proposes that the user has the discretion to either continue in a "normal" connection mode if the "secured" connection mode fails or to establish another secured connection. For example, Abdo states in Paragraph 67 as follows (with emphasis added):

In either case, before returning to a NORMAL connection, the user will be notified that the attempt to establish a SECURED connection has failed and given the choice to conduct another attempt to establish a SECURED connection, or instead acknowledge the return to a non-encrypted NORMAL connection.

In contrast, Claim 1 recites that the security core is configured to abort the recording and the transforming when a condition is met, *i.e.*, if one or more of the audio recording component and the at least one transformation component fails to remain operably connected to the security core during the recording of the audio stream and the transforming of the audio stream. Abdo proposes allowing the user discretion to continue in a "normal" mode or attempt to establish another "secure" mode connection. Therefore, Abdo teaches away from a security core that is configured to abort the recording and transforming of the data when one or more of the audio recording component and the transformation component fails to remain operably connected to the security core recited in Claim 1.

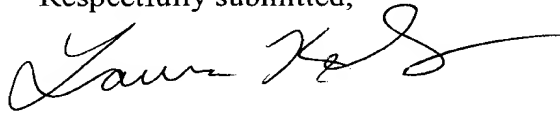
Accordingly the Applicants respectfully submit that Claim 1 is patentable over the cited references. In addition, the Applicants submit that Claims 25 and 49 are patentable for reasons similar to those discussed above with respect to Claim 1. Moreover, Dependent Claims 2-10, 12-24, 26-34, 36-48, 50-58, and 60-71 are patentable at least as per the patentability of Claims 1, 25 and 49 from which they depend.

In view of the above, it is respectfully submitted that this application is in condition for allowance, which action is respectfully requested.

In re: Hind et al.
Application No.: 09/765,127
Filed: January 17, 2001
Page 22

It is not believed that an extension of time and/or additional fee(s)-including fees for net addition of claims-are required. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to our Deposit Account 09-0461.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Laura M. Kelley", with a long horizontal flourish extending to the right.

Laura M. Kelley
Attorney for Applicants
Registration No. 48,441

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

Wireless Secure Device

Authors: Samer Abdo, Rolf Ambuehl, Olivier Bodenmann

The present invention includes a set of processes for establishing a secure radio-frequency ("RF") data link (or a secure link) between wireless devices, e.g., a keyboard or a pointing device, and its receiver. A secure connect process allows a predetermined number of receivers, e.g., one receiver, to connect to at least one device, e.g., a keyboard, at a time, while reducing the probability that an unwanted link to another receiver cannot be established to a negligible level. A data encryption/decryption process provides data privacy over the RF link.

The present invention also includes a software module that may be resident on a host personal computer to display a key that may be entered into a device, e.g., a keyboard, to assist with the establishment of a secured link. The software module may also assist with guiding a user throughout the secure link process and monitoring a status of the secured link as well as warning the user if the security mode is switched off without permission being granted.

Features of the present invention include:

- Allowing for multiple connection modes of which at least one provides a secure connection. For example, the present invention provides a system and a method to ensure that a given device, e.g., a keyboard, cannot get connected through a RF-link to a receiver other than the one to which it is intended to be connected. This may be referred to as a "Secure Connect" operation. The present invention alternatively allows for a connection between devices, e.g., a keyboard, and one or more receivers. This may be referred to as a plain "Connect." operation.
- Using a data encryption system and method for the wireless transmission that provides substantial protections against eavesdropping (malicious or accidental), without demanding or taxing processing resources and impairing the responsiveness of the system in a substantially detectable way.
- Shielding a user from inconveniences as a result of an encryption system or method. For example, a user may be shielded from the inconvenience caused by desynchronization between a device, e.g., a keyboard, and receiver, which would result in wrongly decoded characters.
- Providing additional security through the wireless device itself. For example, sensitive data such as a device (e.g., keyboard) identifier (referred to as "Short_ID" in one embodiment) and an encryption key may be generated internally by the devices, making a user unable to force a given value to the identifier and the key.
- Keeping a user informed on a status of the data link: e.g., SECURED link (or mode) or NORMAL link (or mode). As an example, a default mode shall be NORMAL, to still allow easy, hassle-free connection. In another example, a SECURED mode may be set when a user desires. A user may switch from one mode to another mode. In one embodiment a user may switch without additional installed software assistance. In another embodiment, software may be included to "legalise" a switch from a SECURED to NORMAL mode.
- In one embodiment, a system and a method for establishing a secure link in accordance with the present invention may be configured with a unidirectional RF link from a device, e.g., keyboard or pointing device, to a receiver. In this case, no reply or "back" transmission may

be needed. In another embodiment, a system and a method in accordance with the present invention may be configured with bi-directional RF link between a device and a receiver.

The above features of the present invention may be provided individually or in whole or part combination to provide a user with security and ease of use.

Background of the Related Art

Wireless devices, e.g., keyboards, pointing devices, etc., operating in lower radio frequency bands, typically (but not restricted to) under 100 MHz, e.g., 27MHz, generally use a conventional system of identifiers (Short_ID) to try to ensure data privacy. However, these conventional systems are vulnerable to eavesdropping, either accidentally or maliciously.

- As an example, if done accidentally, a user may be subject to a probability of 1 over 4095 that the user's wireless device has the same identifier ("ID") as a neighboring wireless device operated by, for example, that same user or another user. This probability is based in part on the Short_ID having a length of 12 bits.
- As an example, if done maliciously, a user may find that someone may attempt to deliberately connect a second receiver to the user's wireless device to spy on that device, e.g., determine what information is being transmitted from it. An example of how this may occur is by having the deliberately eavesdropping user attempt to connect to the user's device through a connection mechanism that functions between the device, e.g., the keyboard, and the receiver. An example of a connection mechanism is a CONNECT button that establishes a link between a device and a receiver.

Embodiments of the present invention

Normal Connect

Normal connect may be defined as a non-secured connection. It may be established in, for example, one of the following manners:

- In a first example, an "out-of-the-box" connection occurs when a freshly powered keyboard (e.g., batteries just inserted) is in the vicinity of a "blank" (e.g., never connected) receiver. Here, no action may be required from a user. The keyboard sends status messages requesting a connection during 30 minutes after the batteries have been inserted.
- In a second example, a standard connection when a user uses a connection mechanism that establishes a link between a device and a receiver. For example, in one embodiment, a keyboard and a receiver may include a connection button, e.g., CONNECT, that when depressed generate radio frequency signals recognized by each other so that a link is established within a predetermined time frame, e.g., 10-seconds.

Secure Connect

Once a normal connection has been established, a user may choose to switch to a SECURED mode. A SECURED mode provides a secure connection (called e.g., a Secure Connect). A "Secure Connect" may be used to allow a predetermined number of wireless devices, e.g., one wireless device, to connect with a predetermined number of receivers, e.g., one receiver, at one time. In one embodiment, the "Secure Connect" ensures that a certain keyboard is connected to a particular receiver. Generally, one embodiment of a process for establishing a secure connection includes a user deciding to establish a SECURE mode. The user may either perform a "Secure Connect" on the wireless device, e.g., keyboard, or open a Control Panel on a computer and click on the SECURE button.

DOCS 1126811 5

ACTING ON KEYBOARD FIRST: If the user elects to perform a Secure Connect on the wireless device, a SECURE CONNECT button on a wireless device may be pressed. In one embodiment this button may be dedicated. In some embodiments the normal CONNECT button may be used, and an additional key may also need to be pressed, for example, a keyboard 'Ctrl' key. This causes a status message requesting a "Secure Connect." In some embodiments, a receiver CONNECT button may also be depressed. In each instance a "Secure Connect" signal may be established. This allows the receiver to forward the "Secure Connect request" event to software that opens a Control Panel associated with the wireless device/receiver combination. In one embodiment each time a "Secure Connect" signal is triggered, the wireless device generates a new random Short_ID.

ACTING ON CONTROL PANEL FIRST: If the user elects to act upon a Control Panel, generally software requests to press the wireless device "CONNECT" button. In addition, in some embodiments an additional key may also be pressed, for example, a 'Ctrl' key on a keyboard.

When a Control Panel is used, a user may be requested to enter a 'key' that is displayed on, for example a screen such as a computer monitor or a keyboard display, e.g., LCD. A 'key' is a string of some predetermined number, e.g., 16, of alphanumeric (e.g., numbers, alphabet letters, or some combination thereof) characters. In one embodiment, a key is generated by a receiver, on a random basis. This key then may be reported to the software, which displays it on the screen. In this embodiment, the key is generated when the receiver recognizes a "Secure Connect" message or signal. Also, in this embodiment, the key may be generated randomly inside the receiver, rather than inside another device, e.g., a cordless keyboard. This avoids the key being sent over an RF link, and restricts the knowledge of the key to the person(s) that have direct sight onto the display. Finally, this embodiment prevents being able to force a given key into the receiver. An advantage of this feature is that it prevents duplication of a key into several receivers, thus invalidating the secured locking concept.

In one embodiment, the alphanumeric characters for the key are chosen among the ones which positions do not vary from one keyboard layout to another. In another embodiment, all alphanumeric character may be used, the software being in charge of remapping those having a different position than for example, a conventional Qerty layout. For example, a first eight characters that are typed on the keyboard may be a key, and for this very reason are not sent out but replaced by numbers 0, 1, 2 . . . 7 and reported as "*" by the receiver. When the eight characters have been entered, the key is created from them and a next 8 characters typed are sent encrypted with this new key. The receiver checks that the received characters match the ones displayed on the screen, and when a last character is correctly received, this validates the key. If there is a typing or transmission error a user may redo the Secure Connect on the keyboard and re-enter the key again as described above. It is noted that in one embodiment eight last characters may be used to check whether encryption is working and may be selected to exercise data bits to the maximum possible extent.

Protection against security mode switching

In one embodiment a SECURED mode and a NORMAL mode may coexist within a wireless device/receiver system in accordance with the present invention. This provides a user with flexibility as to which mode to select for operation. For SECURE mode, software allows a user to select a password at their own discretion. The user may be prompted for this password

by the system when the user elects to operate the system in SECURE mode. Once provided, the system can establish a secure connection (or session). If the user elects to no longer operate in a SECURE mode, a switch back to NORMAL may be made by providing to the system the selected password. If the connection switches from SECURE mode to NORMAL mode without the user providing the requisite information, the system will provides a warning back to the user. For example, a software mechanism will flash a warning icon on a screen or an audible warning may be triggered or some combination of both visual and audible warning.

Data Encryption

Generally, standard encryption schemes operate on long blocks of data (for example, 64 to 128 bits). In one embodiment, an encryption scheme may synchronize an encoding scheme of a keyboard with a decoding scheme of the receiver. If this synchronization is lost because of lost transmission packets, the result could be wrongly decoded characters. For example, an "ESC" character from a keyboard could suddenly be decoded as an "ENTER", resulting in an unwanted operation to be performed by a computer. To assist with securing an encryption scheme, a system may send a counter with each encoded character, to keep the receiver synchronized with a sequence. However, in some embodiments a counter may have the same length than the key which causes incompatibility with many RF bandwidth ranges, e.g., approximately 600 to 9600 bits per second (bps) range (e.g., 2400 bps). It is noted that in one embodiment sending a counter used as the encryption source data may create a security ride in the system.

To address this issue in an alternative embodiment a non-sequential, non-standard encryption scheme may be used. A non-sequential, non-standard encryption scheme is not prone to suddenly desynchronize because of lost packets. Moreover, such a scheme uses much less computing resources (e.g., memory and execution time) than the sequential encryption scheme.

Turning now to a general description of one embodiment of an encryption system and method in accordance with the present invention, it is noted that the description will be with reference to a keyboard for ease of understanding. Those of skill in the art will recognize that the principles described are also applicable to other wireless devices.

Generally, there are approximately 127 keys to transmit, although upper codes from 128 to 255 may be set aside for encoding. Moreover, note that in some embodiments some keys may not need to be encrypted, as they may be general function keys or "user keys" such as Internet keys, Multimedia keys or System keys.

In a first stage, the most probable keys (like Space, "e", "a", etc) are "scattered" among a set of upper codes, e.g., 128 upper codes, in such a way that the global histogram of character frequencies are at least partially changed. This makes it difficult to identify an encoded character by its frequency. A result of this operation is a predetermined number of bits, e.g., 8 bits, of scattered data. This data may also be scattered using other conventional techniques.

The bits of the scattered data are mixed with random-like data and are encoded as another set of predetermined bits, e.g., 15 bits, by a non-linear function depending on a predetermined key, e.g., 32-bit key, previously entered by a user. It is noted that the mixing of the random-like data may be conventional. In addition, the application of the non-linear function may also be conventional. In some embodiments, a linear function may be added, combining the predetermined bits, e.g., 15 bits, output with additional predetermined bits, e.g., 15 data bits, selected within the key bits. Those skilled in the art will recognize that the number of bits at

each step of the process may vary according to the chosen embodiment and the security level that has to be reached. For example, encryption may be done on 24 bits rather than 15 bits, to increase data security, but the 15 bits may be considered as a minimum to reach a reasonable security level.

Generally, a typical wireless frame includes data structures such as FRAMETYPE, a DATATYPE, a SHORT_ID, the DATA and a CHECK. In contrast to conventional keyboard formats, a "Scrambled Keyboard Data" format has a shorter frame so that fewer bits, e.g., 15 bits, are transmitted, plus a "KeyDepressed" bit which is not part of the encryption scheme. This results in e.g., 16 bits, rather than, e.g., 11 bits, as defined for conventional KEYBOARD data formats. Moreover, the present invention ENCRYPTED KEYBOARD data type is coded on fewer bits, e.g., 2 bits, rather than more bits, e.g., 5 bits, as used by conventional keyboard data, hence sparing some bits, e.g., 3 bits. Result allows the ENCRYPTED KEYBOARD frame to be overall only two bits longer than the usual KEYBOARD format and is only a few microseconds (e.g., 830 microseconds) differential from a time perspective.

What is encrypted and what is not

In one embodiment, to avoid disclosing any information about the encryption by sending recognizable keys, there is no encoding of the "KeyDepressed" bit and same encryption pattern for both the key "Make" (depressed) and key "Break" (released) are sent in a report. Further, repeated reports concerning a key event may be the same (for example, each key event is sent twice to compensate any RF loss). Refresh reports are sent at some predetermined intervals, e.g., 200ms, to confirm a key depressed status should ideally also be kept identical.

Encryption effectiveness and robustness

The present invention includes a number of advantages/benefits. First, there is only a 1/4095 probability that a receiver other than one intended to communicate with the wireless device will receive the data transmitted by RF. For example, with approximately 250 millions possible keys, the global probability to have the data accepted on another receiver and correctly decrypted is less than 1/1,000,000,000,000 (one over 1000 billions). Moreover, a randomly chosen key by another other receiver in accordance with the present invention is likely to decode only approximately half of the information, the remaining bits being lost in the decryption process because of the wrong key. This makes a statistical attack very likely to fail, as essential information is missing. Even if the wrong key by chance "looses" less bits, a statistical attack on the decoded characters may be defeated due to the "scattering" process described above.

Additional advantages/benefits of the system and method of the present invention is that a user is unable to force a new key into the receiver because it is generated internally on a random basis. This beneficially allows for generating a new key to create a new Secure Connect when spying device enters into the wireless device/receiver combination. Specifically, the claimed invention allows for the internal generation of a new key, which in turn changes the Short_ID, causing the spying device to be disconnected. Moreover, the claimed invention allows for generating a new key that allows the proper wireless device and receiver to establish a communication link between them.

The present invention also provides security advantages in that breaking an RF link encryption needs advanced and costly hardware instrumentation. Further, without knowing how the encryption is done the number of possibilities to encode, for example, 127 keys with, for example, 15 bits codes is huge (about $10^{69.49}$) thereby discouraging any form of a "brute force"

attack. It is noted that the system and method of the present invention includes a security level at least equal to, for example, a 40-bit secret key algorithm. Further, because the Short_ID and the key are generated inside the wireless device, the overall security of the system could be considered as better than prior solutions.

002221 6488209